Office of Liquor and Gaming Regulation

Random number generator minimum technical requirements

Version 1.5

Queensland Government

For further information, please contact the Office of Liquor and Gaming Regulation on 13 QGOV (13 74 68) or visit https://www.business.qld.gov.au/industry/liquor-gaming

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to:

- advise the industry of the Office of Liquor and Gaming Regulation's (OLGR) minimum technical requirements for random number generators (RNGs)
- ensure requirements are consistently applied
- achieve a high standard of integrity of RNGs used in Queensland gaming
- ensure that RNGs used in Queensland are sufficiently random for their intended purpose
- maintain the integrity of gaming in Queensland by ensuring that all RNGs in use are secure for their purpose and that their outcomes are sufficiently difficult to predict under all conditions.

1.2 Scope

This document is applicable to all gaming providers in Queensland. These requirements apply to the technical evaluation of RNGs, submitted for evaluation after the date of publication of this document, by OLGR for use in gambling in Queensland.

1.3 Definitions/abbreviations

Cryptographic random number generator (CRNG)

A type of RNG that produces an entirely unpredictable sequence of numbers

A CRNG is resistant to attack or compromise by an attacker with modern computational resources and/or knowledge of the RNG source code.

Cycle

With respect to a PRNG, the cycle refers to the number of results generated by a PRNG before it starts repeating the previous sequence of raw results.

With respect to a game or application, it refers to the total number of theoretical possible outcomes in the game or application.

Cycling

Refers to the process of continuously obtaining a new raw value from a PRNG and throwing it away without making any use of the value

This is typically done to help prevent the deduction of the current state of a PRNG.

Entropy Gathering

Entropy is needed to seed an RNG and is also used to compliment the state of an operating RNG.

Entropy is the randomness that occurs as the result of a process—for instance, it can be produced by timing the delay between entry key strokes.

Mapping

Refers to the process of selecting an outcome using the result from an RNG

Pseudo-random number generator (PRNG)

A type of RNG implemented in software or firmware that generates a predictable sequence of numbers with the intended property of statistical randomness

PRNGs use a ‘deterministic algorithm’, in that future outcomes are directly dependent on previous outcomes.

Random number generator (RNG)

Refers to any item of hardware or software that can generate random numbers with the intended property of statistical randomness

An RNG may be composed of several other RNGs. Accordingly, the term RNG can also be used to refer to a specific ‘underlying’ RNG within an overall RNG.

The operation of RNGs can be split into these areas: seeding, underlying RNGs, scaling, mapping, cycling and entropy gathering. (**Note:** Not all areas are applicable depending on the type of RNG.)

Range

Refers to the size of the values, and the lowest and highest value, required to determine the outcome

Raw Results

Refers to results from an RNG before any scaling or mapping takes place

Seed

Refers to the initial state information typically required for RNGs and in some cases mechanical RNGs

Seeding

Refers to the process used to initialise the state of the RNG

Scaling

Refers to the methodology used to convert the raw results of an underlying RNG into the required range of output values

An example of this would be where a random number from 1 to 100 is required and the RNG used produces random numbers between 1 and 232. Scaling refers to the process used to convert from the potentially large numbers produced by the RNG into the smaller number range required.

Underlying RNG

The low level RNG used to generate raw results

2 Policy

All RNGs must be submitted to OLGR for evaluation and approval under the following legislation:

- *Casino Control Act 1982*
- *Charitable and Non- Profit Gaming Act 1999*
- *Gaming Machine Act 1991*
- *Keno Act 1996*
- *Lotteries Act 1997*
- *Wagering Act 1998*

3 Categories of random number generators

The following are the categories of RNGs:

- Cryptographic random number generators (CRNGs)
- Pseudo random number generators (PRNGs)
- Mechanical RNGs—a mechanical device used to generate random results excluding hardware RNGs. For example: roulette wheels, dice and ball-draw machines.
- Hardware RNGs (or true RNGs)—these RNGs are devices that generate random numbers from a physical process, often based on microscopic phenomena that generate low-level, statistically random noise signals.

4 Requirements

4.1 RNG submissions

A submission under these requirements must comply with the latest version of the OLGR Submissions Requirements document available from the Queensland Government Publications website.

4.1.1 Submit a fully functional RNG device. If this is not possible, detail the reasons why it is not possible and have a fully functional RNG device available for access by OLGR officers.

4.1.2 In the submission letter, designate the overall submitted RNG with a name and version number for identification purposes.

4.1.3 Submit all scaling and mapping algorithms to be used in conjunction with the submitted RNG. Each of these algorithms must be provided with a unique name or designation and version number.

4.1.4 Supporting references or academic reviews of the RNG and scaling algorithms are desirable if available.

4.1.5 Clearly state in the submission letter the RNG's intended use. This must also be in regard to the frequency of calling, the required result ranges, the expected application cycle requirements, maximum prize size, number of prizes drawn and frequency of draws. (**Note:** The RNGs will be evaluated and approved for use with respect to these items.)

4.1.6 Supply all applicable source code for the overall RNG including scaling and mapping algorithms. Where possible, the source code must be able to be compiled and some sample output data provided to verify it. A method to verify the provided source code is

used, in respect to the live system, may be mandated at OLGR's discretion and depends on overall risk.

4.1.7 Mechanical-based RNGs must be submitted with all custom or non-commercially available equipment/gear/harnesses required to fully test them.

4.1.8 Mechanical-based RNGs must be submitted with all equipment required in order to commission, decommission and operate the device.

4.1.9 Submit the methodology, procedure, time interval and tests performed for any system monitoring which occurs to ensure continuing health of the RNG.

4.1.10 Provide literature that supports the ability of the RNG to produce the required level of random results. If possible, provide links to reviews published on the internet that detail capabilities of or testing done on the RNG.

4.2 General

The following requirements apply to all RNG types except where otherwise stated.

4.2.1 Randomness—RNGs must produce results which can be proven to be:

- statistically independent and pass industry standard statistical tests
- uniformly distributed over the range of results
- unpredictable

4.2.2 The state information of an RNG must be a secret in the overall RNG and not be externally visible or accessible. An exception to this requirement may be granted for publicly available state information that is proven to not compromise in any way the security or integrity of the game using the RNG. For example, for ball drawing RNGs, the state information is the current instantaneous location of the ball in the machine.

4.2.3 The range of values produced by the RNG must be adequate to provide sufficient precision and flexibility when setting event outcome probabilities.

4.2.4 There must be no external mechanism that can affect the outcome of the RNG. For example, there shall be no externally selectable options that alter or affect the RNG.

4.2.5 For RNGs that gather additional entropy over time the source of injected entropy must be demonstrated to be failsafe. For example, the RNG must block if the entropy gathering process fails.

4.2.6 Any RNG used for the game of Keno or similar cycle game and prize game must use a hardware-based RNG combined with other sources of true entropy.

4.2.7 At the application level, random numbers for a game must not be generated (if possible) until all player input choices or bets have been made—that is, the game must be 'closed' first. There must not be any interval where access to the result could accrue a benefit.

4.2.8 The RNG must be secure in proportion to its level of responsibility of its application and the size of the prizes awarded as a result of the RNG outcome—that is, the risk to the integrity of gaming and community impact of fraud in relation to the RNG.

4.3 Hardware RNGs

These are the requirements specific to hardware based RNGs.

4.3.1 Hardware-based RNGs must not be solely used as standalone RNGs but must be combined with other random sources of true entropy. For high risk/value/availability applications, potentially 2 independent hardware-based entropy sources should be combined.

4.3.2 Consideration as to whether the output of the hardware based RNG needs whitening should be given. Usually this is covered by the manufacturer's operating notes.

4.4 Mechanical RNGs

The following are requirements specific to mechanical-based RNGs.

4.4.1 A mechanical RNG must not have any taint, bias or patterns without acceptable and documented fail-safes in place (e.g. periodically rotating canoe rings in roulette wheels). If a product may develop a taint, bias or pattern through wear, the product must be monitored or tested for this on an ongoing basis and a procedure for this must be included in the RNG submission.

4.4.2 Initial starting positions, if any, must not correlate to output positions (e.g. ball drawing devices).

4.4.3 The device must operate correctly if the surface it sits on is not level (if applicable), unless there is an acceptable fail-safe and documented procedure in place to ensure the device remains level during operation.

4.4.4 If possible, mechanical RNGs must be submitted with the ability to be rigged up to enable the device to be auto-played (no manual intervention) and the results automatically electronically recorded for an indefinite period. If this is not possible, results from the RNG under conditions specified by OLGR may be required as a part of the evaluation.

4.4.5 Mechanical RNGs must also be submitted with the following information for evaluation and approval:

- commissioning/decommissioning procedures
- operating procedures
- care and preventative maintenance procedures.

The main requirements for the documents are completeness, correctness and that a non-technical person must be able to follow them. These documents will also be evaluated on the likelihood of the procedures preventing or causing bias or taint to the mechanical device and detecting it if it occurs.

4.4.6 If the device is prone to mechanical wear, especially wear that can adversely affect the randomness of the results, provide documentation or manuals that include the maintenance procedures. The preventive maintenance procedures provided must detail best-practice to reduce the risk of wear occurring and detect any wear that negatively impacts the randomness of the device results.

4.4.7 There may be a requirement imposed to monitor the device to ensure no detectable degradation of randomness occurs during operation.

4.4.8 Results from the RNG must be clear and not open to confusion.

4.4.9 If possible, no mapping of results should be used. Any mappings used must be obvious, unambiguous and clearly visible to players—for example, odd and even results in roulette.

4.4.10 Any ability to tamper with the device in such a way as to affect the results produced should be minimised and controlled. Any attempted tampering must be clearly visible to a casual observer or easily tested for.

4.4.11 Any damage to the device that affects the randomness of the results should, if possible, produce no result and clearly display an error state or visible change to the equipment or the draw process, or be able to be tested for.

4.4.12 Packaging for transportation of the mechanical RNG device must be:

- reusable
- considered sufficient by OLGR's CEO to ensure the device's randomness will not be adversely affected during normal transportation of the device.

4.4.13 In the case of a mechanical RNG, there may also be a maximum lifetime limit imposed or a maximum cycle. This must be documented if applicable.

4.5 Cryptographic RNGs

These are the requirements specific to cryptographic RNGs.

4.5.1 It must be computationally infeasible to predict or estimate future outcomes of the CRNG when previous outcomes are known. This must be ensured through the appropriate use of a recognised cryptographic algorithm.

4.5.2 The CRNG must be resistant to a state-compromise extension attack. In the event that the RNGs state is known, it must either be infeasible to use knowledge of this state to predict future outcomes, or the effective duration of any potential exploit is limited. This is to be achieved by periodically modifying the RNGs state by injecting additional external entropy.

4.6 Seeding

Some RNGs, such as PRNGs, require seeding before use. These requirements apply to RNGs that require seeding.

4.6.1 The seeding process must be a random process in itself, subject to all requirements in this document concerning randomness.

4.6.2 The entropy gathered before seeding must be at least as random as results required during normal operation.

4.6.3 The seeding process must not be visible externally.

4.6.4 The method of seed generation must ensure that when a duplicate of the RNG is used in multiple devices, it is highly improbable that the same initial sequence of random numbers is used in more than one device.

4.6.5 When a PRNG is reseeded is must only be done with a seeding methodology that ensures all PRNG outcomes remain equally probable.

4.6.6 The RNG initial state must be seeded from an entirely unpredictable source of entropy.

4.7 Scaling algorithms

RNGs typically require a scaling algorithm to take a raw value from the underlying RNG and convert it into the desired range required by the application. The requirements in this section apply to any scaling algorithms used in an RNG.

4.7.1 The scaling algorithms must achieve their intended results without bias or with an insignificant amount of bias.

4.7.2 Each of the possible outcomes of the scaling algorithm must have the correct desired probabilities as per the mathematical model of the game or application.

4.7.3 Scaled results must pass all tests for randomness, as well as the raw RNG results.

4.8 RNG monitoring

Monitoring is a broad term, and in the simplest sense any RNG monitoring that is implemented should only be done so to add safeguards to the ongoing operation of the RNG. Care should be taken to ensure monitoring does not introduce risk of compromising the core RNG operation or its randomness.

4.8.1 Hardware RNGs must be monitored. Such monitoring must only be implemented in accordance with the RNG manufacturer specifications and be appropriate to the context of their operation within a device. Monitoring should aim to confirm that an RNG continues to perform acceptably and has not deteriorated over time.

4.9 Charitable and non-profit gaming RNGs

4.9.1 An RNG which forms part of another commercially available product, where the source code is not available for submission to OLGR, may be approved for use under the Charitable and Non-Profit Gaming Act provided that:

- the process for generating randomness that the commercially available product implements, is known
- the commercially available product is a well-known product with a demonstrated track record

4.9.2 For electronic draw systems used for category 3 games, the following requirements apply.

- Software that has been identified as regulated gaming equipment must be verifiable and must be achieved using a secure hash at a minimum, such as a hash list of individual binaries or compiled images, or an overall hash of the regulated gaming equipment.
- The draw system must include a draw file that will be restricted from any change once draw closure occurs. This draw file must be immediately secured from any attempted changes and must contain the draw parameters used in the draw, e.g. Number of Tickets, Total Ticket sales, Draw No and other information imperative to the draw. This file must be write-protected and immediately copied to a secure location for archiving that requires increased security clearance to be able to access the file. A log indicating file access (read/write) attempts must be implemented and this log must be readily available. Draw closure is the state of the draw where no more tickets are to be issued by the electronic draw system.
- The draw system must be capable of producing a log as a result of the draws performed. Changes to log entries must not occur, and any attempts of alterations to the log entries must be entered as a log entry. The system must be able to authenticate

that these logs have been created by the draw system using a secret (i.e. a digital certificate).

- The draw system must have an interface that will allow it to provide the draw results, logs etc. via a secure process without any manual procedures being required.

4.9.3 OLGR recommends that charitable and non-profit draw system providers also consider a decentralised draw system to cater for any art union draws that have a potential of high risks (large value prizes). Learn more at www.publications.qld.gov.au/dataset/decentralised-draw-systems

5 Revision history

Version	Changes	Who	Release date	Incept date
1.2	Release for industry comment	CH & RL	14/03/2006	
1.3	Minor update to incorporate feedback from industry	CH	15/06/2006	
1.4	Updated to new DEEDI report document template	YL	20/08/2010	
1.4.1	Updated to new DJAG report document template	JG	19/4/2016	
1.5	• Minor updates to existing requirements • Additional requirements for cryptographic specific RNGs • Additional requirements for Charitable and Non-Profit Category 3 draws • Updated to new DJAG report document template	NJ	30/9/2020	